MASTER OF SCIENCE
IN
SYSTEMS ENGINEERING

APPLICATION AND EVALUATION OF HIGHER ORDER CYCLOSTATIONARY TECHNIQUES IN SIGNAL CLASSIFICATION

Glenn A. Barker-Lieutenant Commander, United States Navy
B.S., United States Naval Academy, 1989
Master of Science in Systems Engineering-September 1999
Advisors: Tri T. Ha, Department of Electrical and Computer Engineering
Vicente C. Garcia, National Security Agency Cryptologic Chair
Chad M. Spooner, Mission Research Corporation

Manmade signals exhibit certain characteristics that are not recognizable using the classic methods of signal processing. Signals that exist within the noise threshold or overlap in time and frequency present an additional challenge because the combination of their features tends to obscure the details of any one signal in the band of interest. However, it has been shown that the features of these signals can be revealed and used to aid in the detection and classification of signals of interest by using higher order cyclostationary (HOCS) methods. In this paper, cyclostationarity will be defined, likely features of signals of interest will be discussed, and a series of evaluations will be conducted and analyzed using the HOCS Based Classifier (HBC) software.

DoD KEY TECHNOLOGY AREAS: Command, Control, and Communications, Computing and Software, Electronics, Sensors, Other (Information Warfare, Information Operations)

KEYWORDS: Cyclostationary, Cyclostationarity, Digital Signals, Signal Classification, Signals Intelligence (SIGINT)

CISCO INTERNETWORKING OPERATING SYSTEM SECURITY VULNERABILITIES (U)

Jonathan J. Bartel-Lieutenant, United States Navy
B.S., University of Wisconsin, 1991
Master of Science in Systems Engineering-September 1999
Advisors: Vicente C. Garcia, National Security Agency Cryptologic Chair
CAPT James R. Powell, USN, Information Warfare Academic Group

The current rapid pace of technological change being experienced while operating in the Information Age is facilitating a convergence of telecommunication, computer, and computer network technologies. In the not too distant future nearly all communications will use computer network components. The key component of internetworking architecture is the router, which is little more than a specialized computer designed for traffic management. As such, a router is dependent upon operating system software, as with any other computer, in order to perform its function. This often leaves routers vulnerable to the same kinds of computer network attacks that have been conducted against traditional operating systems such as UNIX and Microsoft Windows NT. The routers of one company, Cisco Systems Inc., dominate the internetworking market. Cisco routers use a proprietary operating system, the Cisco Internetworking

Operating System (IOS). This thesis investigates some potential Cisco IOS security vulnerabilities that may lead to compromise of the router.

DoD KEY TECHNOLOGY AREA: Computing and Software

KEYWORDS: Computer, Router, Computer Network, Computer Security, Cisco IOS

METHODS FOR MITIGATING VULNERABILITIES OF NETWORK-LEVEL ENCRYPTION IN ATM NETWORKS (U)
Orman K. Fuller-Commander, United States Navy
B.S., East Carolina University, 1981
Master of Science in Systems Engineering-September 1999
Advisor: John C. McEachen, Department of Electrical and Computer Engineering
Second Reader: Linden Mercer, Naval Research Laboratory

Abstract is classified.

DoD KEY TECHNOLOGY AREAS: Command, Control, and Communications, Other (Intelligence)

KEYWORDS: Vulnerabilities of Network-Level Encryption, ATM Networks, FASTLANE, KG-75, KG-189, SONET

MONITORING INFORMATION SYSTEMS TO ENFORCE COMPUTER SECURITY POLICIES
Scott W. Graham-Lieutenant, United States Navy
B.G.S., Roosevelt University, 1989
Master of Science in Systems Engineering-September 1999
and
Stephen E. Mills-Lieutenant, United States Navy
B.S., Old Dominion University, 1992
Master of Science in Systems Engineering-September 1999
Advisor: Vicente C. Garcia, National Security Agency Cryptologic Chair
Second Reader: James B. Michael, Department of Computer Science

Many computer security policies are written relatively vaguely. In many ways this is intentional to allow for easier access to all the functionality of the computer network. However, too much leeway allows users, without a need to access many of the network functions, the ability to execute functions that might cause harm to the system or provide access to information they have no need to see. With this in mind, this paper takes a look at computer security. We start with a brief history of computer security and continue with a look at internal security. Since our focus is on computer misuse and detection, a look at internal security provides a look at the reasons why we should attempt to monitor the activities of users. Misuse detection requires at least two features. These are audit reduction and profiling ability. When audit features are enabled in the operating system, massive files can build up. By establishing profiles of personnel usage, the automated audit features can quickly scan audit files, look for usage that falls outside what is determined to be normal, notify administrators, and delete old audit data. A misuse detection system, such as the Computer Misuse Detection System marketed by ODS Networks, may be implemented and incorporated into a comprehensive security policy.

DoD KEY TECHNOLOGY AREA: Computing and Software

KEYWORDS: Computer Security, Profiling, Computer Security Policy

INVESTIGATION OF MINIMUM RESOLVABLE TEMPERATURE DIFFERENCE FORMULATION FOR POLARIZED THERMAL IMAGING RANGE PREDICTION

Edson Fernando da Costa Guimarães-Captain, Brazilian Air Force
B.S., Brazilian Air Force Academy, 1990
Master of Science in Systems Engineering-September 1999
Advisors: Alfred W. Cooper, Department of Physics
Ronald J. Pieper, Department of Electrical and Computer Engineering

Previous measurements have demonstrated that a polarization filter can increase ship-background temperature contrast in the infrared, while decreasing the received radiance. Application of this technique to increasing range for detection or recognition of ship targets is being investigated through detection range modeling for a generic FLIR sensor. Laboratory measurements have been made of effective Minimum Resolvable Temperature Difference (MRTD) of a serial-scan 8-12 μm sensor for polarized and unpolarized radiation. A variety of standard four-bar target boards of varied spatial frequency and controlled bar-background temperature difference were used to construct MRTD versus spatial frequency. Results were compared with model predictions using known or measured component parameters for the AGA-780 imager, showing close agreement for observations made by a "trained observer." A modified form of MRTD was developed for a polarized target using a reformulation of the thermal derivative of Planck's law. Modeled and measured values agreed closely for the unpolarized case, and also for both vertically and horizontally polarized cases when the appropriate parameters of the polarization filters were included. Mathematical analysis and measurement agreed in displaying an increase in MRTD with polarization. Predictions of maximum detection and recognition ranges using estimates of polarized effective target-background temperature difference indicated probable range improvement for sea surface degree of polarization in excess of 20%.

DoD KEY TECHNOLOGY AREAS: Battlespace Environments, Electronic Warfare, Sensors, Modeling and Simulation

KEYWORDS: Thermal Imaging Systems, Minimum Resolved Temperature Difference, Polarization Filters

TELEMETRY AND GPS ANTENNAS FOR A MICRO AIR VEHICLE

Emin Guven-Turkish Navy
B.S., Turkish Naval Academy, 1993
Master of Science in Systems Engineering-September 1999
Advisor: David C. Jenn, Department of Electrical and Computer Engineering
Second Reader: D. Curtis Schleher, Information Warfare Academic Group

This thesis presents telemetry and GPS antenna designs for a Micro Air Vehicle (MAV). The telemetry antenna type is selected as a monopole, which is to be mounted under the bottom of MAV. A prototype of the telemetry antenna was designed, built, and tested at 2.45 GHz. For the GPS antenna, several types of antennas were examined. Helix, conical spiral, tripole, and crossed-dipole antenna types were designed and simulated using computer software. Additionally, microstrip and slotted-ring antenna types were presented. The antenna computations were performed using the Numerical Electromagnetics Code (NEC).

DoD KEY TECHNOLOGY AREAS: Air Vehicles, Electronics, Sensors

KEYWORDS: GPS Antennas, Telemetry Antennas, Micro Air Vehicle, NEC

PUBLIC KEY INFRASTRUCTURE (PKI) INTEROPERABILITY: A SECURITY SERVICES APPROACH TO SUPPORT TRANSFER OF TRUST

Anthony P. Hansen-Lieutenant, United States Navy
B.S., University of Notre Dame, 1990
Master of Science in Systems Engineering-September 1999
Advisor: James B. Michael, Department of Computer Science
Second Reader: Timothy J. Shimeall, Department of Computer Science

Public key infrastructure (PKI) technology is at a primitive stage characterized by deployment of PKIs that are engineered to support the provision of security services within individual enterprises, and are not able to support the vendor-neutral interoperability necessary for large, heterogeneous organizations such as the United States Federal Government. Current efforts to realize interoperability focus on technical compatibility between PKIs. This thesis defines interoperability as the capacity to support trust through retention of security services across PKI domains at a defined level of assurance and examines the elements of PKI interoperability using this more comprehensive approach.

The initial sections discuss the security services PKIs support, the cryptography PKIs employ, the certificate/key management functions PKIs perform, and the architectural elements PKIs require. This provides the framework necessary for discussing interoperability. Next, the two fundamental aspects of interoperability, technical and functional, are presented as well as their constituent elements and the existing barriers to interoperability. Finally, the proposed U.S. Department of Defense and Federal Government PKI architectures are analyzed and recommendations made to facilitate interoperability.

DoD KEY TECHNOLOGY AREAS: Command, Control, and Communications, Computing and Software, Other (Information Assurance)

KEYWORDS: Cryptography, Public Key Infrastructure, Computer Security, and Information Warfare – Protect

MODELING AND INFLUENCING IRAQ'S USE OF BIOLOGICAL WEAPONS (U)

Robert Macky-Lieutenant, United States Navy
B.A., Auburn University, 1991
Master of Science in Systems Engineering-September 1999
Advisor: CAPT James R. Powell, USN, Information Warfare Academic Group
Second Reader: LT Raymond R. Buettner, Jr., USN, Information Warfare Academic Group

After the Persian Gulf War, the United Nations Special Commission (UNSCOM) was delegated the authority to destroy, remove, or render harmless all material associated with Iraq's biological weapons (BW) program. However, after several years of cat-and-mouse games with UNSCOM, Iraq has been able to keep most of its BW program viable. Does Iraq intend to use BW?

Utilizing a computer program known as Situational Influence Assessment Module (SIAM), an influence net model is constructed to ascertain the probability of Iraq using BW. SIAM also has the ability to locate weaknesses revealed by the model, known as pressure points, which are vulnerable to influences that may affect Iraq's determination to use BW or from further developing its BW program. Various options, including Information Operations (IO), were designed and tested against selected pressure points to identify those options most likely to prevent Iraq from continuing down its current path as predicted by the model.

DoD KEY TECHNOLOGY AREA: Modeling and Simulation

KEYWORDS: Iraq, Biological Weapons, Biological Agents, Biological Warfare, IO Modeling and Simulation, SIAM, Modeling and Simulation, Information Operations

MODELING A HIGH POWER MICROWAVE (HPM) WEAPON SYSTEM (U)

Benjamin R. Nicholson-Lieutenant, United States Navy
B.S., United States Merchant Marine Academy, 1993
Master of Science in Systems Engineering-September 1999
Advisors: Michael A. Morgan, Department of Electrical and Computer Engineering
CAPT James R. Powell, USN, Information Warfare Academic Group

The objective of this research was to model the electromagnetic output of a proposed High Power Microwave (HPM) weapon system. Based on the computer simulation, the proposed weapon system should produce the desired electromagnetic energy levels and lethality patterns necessary for mission accomplishment. The simulations also exposed possible air ionization problems that warrant further investigation.

The antenna data was generated using GNEC, a method of moment's computational electromagnetic code. The proposed excitation method was modeled using an electrical circuit equivalent created in MATLAB 5.3, a mathematical matrix computational program. The final system results were also produced using MATLAB.

DoD KEY TECHNOLOGY AREAS: Electronic Warfare, Directed Energy Weapons, Modeling and Simulation

KEYWORDS: Electronic Warfare, Directed Energy Weapons, Antenna Design, Antenna Modeling, Electromagnetic Simulation

WIRELESS LOCAL AREA NETWORK (WLAN) APPLICATIONS IN THE COMMON AVIATION COMMAND AND CONTROL SYSTEM (CAC^2S)

Leslie M. Prior-Captain, United States Marine Corps
B.S., Texas A&M University, 1990
Master of Science in Systems Engineering-September 1999
Advisors: Syed R. Ali, Defense Information Systems Agency Chair
CAPT James R. Powell, USN, Information Warfare Academic Group

The United States Marine Corps has begun to develop a new aviation command and control system that will replace the existing stove-piped systems. The Common Aviation Command and Control System (CAC^2S) program seeks to leverage advances in technology to field a system that supports Operational Maneuver from the Sea (OMFTS) and the Marine Corps doctrine of maneuver warfare. To meet the demands of OMFTS and maneuver warfare the CAC^2S must provide a high degree of flexibility, mobility, and responsiveness in a rapidly evolving environment.

This thesis focuses on the application of available Commercial-off-the-Shelf (COTS) Wireless Local Area Network (WLAN) technology that meets the operational requirements of OMFTS and maneuver warfare without degrading the capabilities of the Marine Air Command and Control System (MACCS) agencies. The various protocols, standards, and technologies common to telecommunications and computer networks are discussed in terms of their suitability in a CAC^2S application. A scenario driven technology demonstration is conducted to analyze the feasibility of the WLAN application. The conceptual objective of a WLAN enabled CAC^2S is to provide the necessary mobility to the MACCS while maintaining situational awareness and the ability to command and control Marine Corps aviation assets.

DoD KEY TECHNOLOGY AREAS: Command, Control, and Communications, Electronics, Electronics Warfare, Other (Wireless Local Area Networks (WLAN))

KEYWORDS: Common Aviation Command and Control System (CAC^2S), Wireless Local Area Network (WLAN), Commercial-off-the-Shelf (COTS), Marine Air Command and Control System (MACCS)

ANALYSIS AND VULNERABILITIES OF SPREAD SPECTRUM WIRELESS LOCAL AREA NETWORKS ON SURFACE AND SUB-SURFACE COMBATANTS

Mark W. Roemhildt-Lieutenant, United States Navy
B.S., University of Wisconsin, Madison, 1991
Master of Science in Systems Engineering-September 1999
Advisor: Xiaopang Yun, Department of Electrical and Computer Engineering
Second Reader: Vicente C. Garcia, National Security Agency Cryptologic Chair

This research effort discusses data transfer over Local Area Networks (LAN) that utilizes a wireless transmission medium. The Wireless Local Area Network standard, IEEE 802.11, utilizes two major spreading schemes in the form of Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS) techniques. This thesis addresses and compares these two spreading schemes.

Naval vessels pose unique transmission difficulties due to the inherent multi-path environment within the skin of the ship as well as the security risks corresponding with the potentially hazardous area in which they must operate. Research was conducted in order to determine how effective and vulnerable an IEEE 802.11 compliant Wireless LAN (WLAN) network would be on a surface and sub-surface combatant.

WLAN's also pose several vulnerability issues that may jeopardize the information being transmitted. This thesis addresses vulnerability and exploitability issues as well as security and encryption methodologies.

DoD KEY TECHNOLOGY AREAS: Command, Control, and Communications, Computing and Software

KEYWORDS: Wireless Local Area Networks (WLAN), IEEE 802.11, Computer Network Vulnerabilities, Encryption

DEVELOPMENT OF A HIGH POWER MICROWAVE UNINHABITED COMBAT AIR VEHICLE (U)

Theodore B. Sanders-Lieutenant, United States Navy
B.S., Auburn University, 1992
Master of Science in Systems Engineering-September 1999
and
Jung Y. Suh-Lieutenant, United States Navy
B.S., University of Maryland, 1990
Master of Science in Systems Engineering-September 1999
Advisor: CAPT James R. Powell, USN, Information Warfare Academic Group
Second Reader: David C. Jenn, Department of Electrical and Computer Engineering

Recent advances in high power microwaves (HPM), especially in source development, prime power, and antenna design, create emergent possibilities for new warfare applications. One area of interest is the use of HPM in conjunction with Uninhabited Combat Air Vehicles (UCAVs). An HPM system integrated with a UCAV would have the ability to upset or damage critical electronic systems in key targets such as leadership or command and control facilities. This paper will present the results of a feasibility and conceptual design study incorporating a high power microwave system into a UCAV. The overall objective is to determine whether the technology exists today for a weapon system of this type and whether inevitable advances in these technologies will result in future systems using this concept.

DoD KEY TECHNOLOGY AREAS: Conventional Weapons, Directed Energy Weapons

KEYWORDS: High-Power Microwaves (HPM), Uninhabited Combat Aerial Vehicle (UCAV), Magnetically Insulated Line Oscillator (MILO), High Frequency Structure Simulation (HFSS)

INTRUSION DETECTION ON THE DIGITAL BATTLEFIELD
Wayne F. Slocum-Lieutenant, United States Navy
B.S., Arizona State University, 1988
Master of Science in Systems Engineering-September 1999
Advisors: Vicente C. Garcia, National Security Agency Cryptologic Chair
CAPT James R. Powell, USN, Information Warfare Academic Group

With the inception of Presidential Decision Directive 63, the nation realized the need to protect its critical infrastructure from a cyber-attack. Together with the IT-21 initiative, the Navy began a journey into the information age that situates itself against a new adversary - the computer hacker. IT-21 designates Microsoft Windows NT 4.0 as the network operating system for tactical and administrative networks and is already being deployed. With NT 4.0 in place and its follow-on, Windows 2000 currently in beta testing, the Navy's networks are potentially plagued with vulnerabilities. However, there are methods to significantly reduce this risk such as securely configuring Windows, using firewalls as well as using vulnerability assessment tools to detect potential weaknesses. Even with these additional measures, it is essential to employ an intrusion detection system. An intrusion detection system is the first warning that a security policy has been breached. This research examines the different methods of implementing intrusion detection systems on the new digital battlefield.

DoD KEY TECHNOLOGY AREA: Other (Information Warfare, Computer Network Defense)

KEYWORDS: IT-21, Computer Network Defense, Windows NT 4.0, Network Intrusion Detection

SECURELY MIGRATING TO WINDOWS 2000
Raymond Tortorelli-Lieutenant, United States Navy
B.S., United States Naval Academy
Master of Science in Systems Engineering-September 1999
Advisors: Vicente C. Garcia, National Security Agency Crytologic Chair
CAPT James R. Powell, USN, Information Warfare Academic Group

IT-21 standards designated Microsoft Windows NT 4.0 as the computer network operating system for tactical and administrative networks. Windows 2000 will be the follow-on operating system used by the Navy and as the Navy transitions to this operating system, a number of vulnerabilities may be discovered. To reduce these vulnerabilities, aggressive testing of the Windows 2000 Beta III is necessary. This will better prepare the Navy and other services for a smooth and secure migration to Windows 2000. Microsoft, in fact, strongly recommends that a test lab be set up to verify this upgrade process for all possible scenarios and to ensure a high degree of success with actual deployments. Command policies regarding defense against disruption and deception of a distributed command information system operating in the Windows 2000 environment can be developed and tested using Windows 2000 Beta III in the Naval Postgraduate School's Computer Network Research Lab (CNRL).

DoD KEY TECHNOLOGY AREA: Computing and Software

KEYWORDS: IT-21, Computer Network Attack, Windows 2000, Computer Security, Migration

AN AIRBORNE HIGH DATA RATE AND LOW COST DIGITAL COMMUNICATIONS NETWORK USING COMMERCIAL-OFF-THE-SHELF WIRELESS LOCAL AREA NETWORK COMPONENTS

Stephen J. Tripp-Lieutenant, United States Navy
B.A., Villanova University, 1991
Master of Science in Systems Engineering-September 1999
Advisors: CAPT James R. Powell, USN, Information Warfare Academic Group
Dan C. Boger, Command, Control, Communications, Computers, and Intelligence Academic Group

Certain National and Navy tasked missions require the rapid dissemination of available data to multiple disparate platforms. Current COTS technologies can provide for the transmission of such data, using lightweight, low cost ground stations to and from airborne platforms. Additionally, Navy ships and other units with existing large bandwidth communications pipelines can provide and share such with accompanying units using the developed high bandwidth, medium range system. This architecture provides LPD communications for deployed forces with sufficient bandwidth and range to allow for rapid exchange of time critical intelligence and communications both to and from remote locations without the benefit of significant indigenous infrastructure and with minimal possibility of compromise. The small, highly transportable nature of wireless LAN components, combined with the spread spectrum nature of their transmissions makes them desirable as an immediate solution to real-time data sharing requirements.

The objective of this work is to apply a systems engineering process to the selection, evaluation and implementation of a COTS wireless computer network. Both computational and experimental models are analyzed to provide a method for selection and verification of system performance. In-flight evaluation demonstrates the ability to transmit and receive high bandwidth data using the optimized system in a realistic operational environment.

DoD KEY TECHNOLOGY AREAS: Command, Control, and Communications, Computing and Software, Other (Information Warfare)

KEYWORDS: Command, Control Communications, and Intelligence, Wireless LAN, Communications, Information Warfare, Computer Networking, Spread Spectrum, IEEE 802.11, Net-Centric Warfare

INTRODUCTION OF NON-TRADITIONAL NETWORK SECURITY SOLUTIONS TO IT-21

Kelvin L. Upson-Lieutenant, United States Navy
B.S., United States Naval Academy, 1991
Master of Science in Systems Engineering-September 1999
Advisors: Vicente C. Garcia, National Security Agency Cryptologic Chair
CAPT James R. Powell, USN, Information Warfare Academic Group

The Information Technology for the 21st Century (IT-21) initiative is second in priority in the Department of the Navy Chief Information Officer's (DONCIO) Office, only to the Year 2000 (Y2K) conversion effort. IT-21, which is the installation of network-ready state of the art computers onboard Navy ships and shore installations, is achieved by adhering to the DON Information Technology Standards Guidance (ITSG). To fully implement IT-21 Defense in Depth strategy, this research will recommend a process to ensure individual systems are secure when fielded, and will address key interface and security issues of Microsoft Proxy Server 2.0 when migrating from Microsoft Windows NT 4.0 to Microsoft Windows NT 5.0 (Windows 2000) Beta 3.

While perimeter network defenses will continue to play an important role for information protection, relying on perimeter firewalls and proxy servers alone to protect an already secure network is not adequate security solution. Non-traditional network security solutions for information systems should be addressed by DON to counter ubiquitous non-traditional attacks by insider and outsider threats. Commercial software such as "Cyberwalls," "Recluse," and "PCFirewalls" may be the network access control solutions for the future.

DoD KEY TECHNOLOGY AREA: Computing and Software

KEYWORDS: IT-21, Firewalls, Proxy Server, Windows 2000